DETAILED ACTION

1.   Claim 26 is objected to because it has two ending period. Appropriate correction is

required.

2.   Claim 20 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the

written description requirement. The claim(s) contains subject matter which was not described

in the specification in such a way as to reasonably convey to one skilled in the relevant art that

the inventor(s), at the time the application was filed, had possession of the claimed invention.

In particular, the recitation "generating the first pseudo-random value from a previously

chaos-based pseudo-random value generated before the first chaos-based pseudo-random value"

in claim 20 is not supported by the specification.

3.   Claims 1-10 and 13-27 are rejected under 35 U.S.C. 101 because the claimed invention is

directed to non-statutory subject matter.

Claims 1-10 and 15-25 are clearly directed to a method. In order for a method to be a

patent eligible process under 35 USC 101, the method must (1) be tied to another enumerated

statutory category (such as a particular apparatus) or (2) transform underlying subject matter

(such as an article or materials) to a different state or thing. (See *Diamondv. Diehr,* 450 U.S. 175,

184 (1981); *Parker* v. *Flook,* 437 U.S. 584, 588 n.9 (1978); *Gottschalk v. Benson,* 409 U.S. *63,*

70 (1972); *Cochrane* v. *Deener,* 94 U.S. 780,787-88 (1876)). Since in claims 1-10 and 15-25 fail

to tie the method to another enumerated statutory category and the method clearly does not

transform a subject matter such as an article or material to a different state or thing, claims 1-10

and 15-25 are clearly directed to a non-statutory process.   The recitations "storing said chaos-

based pseudo-random sequence (Xn) in a circuit" in claim 1, and "storing the first chaos-based

pseudo-random value in a circuit" in claim 15 are mere insignificant post-solution activity (in re

Bilski), and thus fail to render claimed invention statutory.

Claims 13,14,26 and 27 are directed to an invention that merely performs calculations

and manipulations of data. In order for such a claimed invention that merely performs

calculations and manipulations of data to be statutory, the claimed invention must accomplish a

practical application, and is not directed to a preemption of a calculation and/or manipulation

data . That is the claimed invention must transform an article or physical object to a different

state or thing, or produce a useful, concrete and tangible result and not cover every substantial

practical application . See State Street 47 USPQ2d, Benson 175 USPQ , and "Interim

Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility", OG

Notices: 22 November 2005. It is clear from claims 13,14,26 and 27 that the invention merely

performs calculations and manipulations of data. The claimed invention does not perform any

physical transformation. The inputs are numbers and the output is also a number. Further, the

result of the invention is a mere numerical value without a practical application recited in the

claims to make the result to have real world value. Thus, the result is not useful, concrete and

tangible. The recitations "operable in an encryption application" in claims 13 and 14, and

"operable to be used in an encryption application", recited in claims 26 and 27 clearly do not

limit the invention to an encryption application. Therefore, the claimed invention is directed to

non-statutory subject matter as the claimed invention fails to accomplish a practical application.

Further, since the claims appear to cover every substantial practical application, they are also

directed to a preemption of the claimed manipulation and calculation of data.

4.   Claims 1-3,5-7 and 15-27 are rejected under 35 U.S.C. 102(e) as being clearly anticipated

by Butler (6,678,707)

        As per claims 1,15,16,18,19,21,26 and 27, Butler discloses in figure 8 a generation of a

chaos-based pseudo-random sequence in an encryption application, including defining a chaotic

map (402-412) for generating a pseudo-random sequence of integer numbers in a certain interval,

choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and

generating numbers of the pseudo-rand sequence, defining a function (800) on the interval whose

inverse has a plurality of branches and calculating numbers of a chaos-based pseudo-random

sequence by applying the function to corresponding integer numbers of the of the pseudo-

random sequence as claimed.

        As per claims 2, 5 ,6,17,24 and 25, Butler disclose in col. 8, lines 18-20, the function

being also exclusive-or function as that of the present invention and thus the inverse of the

function has a number of branches equal to the largest bound of the interval.

        As per claims 3,7, 22 and 23 Butler discloses in figure 3 the chaotic map a truncated

linear congruential generator.

5.   Claims 1-3,5-7 and 15-27 are rejected under 35 U.S.C. 102(e) as being clearly anticipated

by Smeets (6,813,625)

        As per claims 1,15,16,18,19,21,26 and 27, Smeets discloses in figure 2 a generation of a

chaos-based pseudo-random sequence in an encryption application including defining a chaotic

map (201) for generating a pseudo-random sequence of integer numbers in a certain interval,

choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and

generating numbers of the pseudo-rand sequence (Z), defining a function F(203) on the interval

whose inverse has a plurality of branches and calculating numbers of a chaos-based pseudo-

random sequence by applying the function to corresponding integer numbers of the of the

pseudo-random sequence as claimed.

As per claims 2, 5 ,6,17,24 and 25, Smeets in col. 6, lines 1-5, the function F being also

exclusive-or function (mod2 sum) as that of the present invention and thus the inverse of the

function has a number of branches equal to the largest bound of the interval.

As per claims 3,7, 22 and 23 Smeets discloses col.5, , lines 45-67 the chaotic map a

truncated linear congruential generator.

6.   Claims 11 and 12 are objected to as being dependent upon a rejected base claim, but

would be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims.

7.   Applicant's arguments filed on 08/12/2008 have been fully considered but they are not

persuasive.

Regarding the rejection of claim 20 is rejected under 35 U.S.C. 112, first paragraph, it is

respectfully submitted that the paragraph [54] discloses that the generation a pseudo-random

sequence of bits is easily repeated for generators of sequences of pseudo-random numbers.

However, it has never disclosed a generation of a pseudo-random value based on a previously

chaos-based pseudo-random value. Therefore it does provide support for "generating the first

pseudo-random value from" as recited in the claim.

Regarding the rejection under 35 U.S.C. 112, it is respectfully submitted that the

recitations "storing said chaos-based pseudo-random sequence (Xn) in a circuit" in claim 1, and

"storing the first chaos-based pseudo-random value in a circuit" in claim 15 are mere

insignificant post-solution activity, and thus fail to render claimed invention statutory (in re

Bilski). Further, the recitations "<u>operable</u> in an encryption application" in claims 13 and 14, and

"<u>operable</u> to be used in an encryption application", recited in claims 26 and 27 clearly do not

limit the invention to an encryption application or a practical application to produce a useful,

concrete and tangible result or to transform an article or physical object to a different state or

thing, and not to cover every substantial practical application.

Regarding the rejection of claims 1-3,5-7 and 15-27 are rejected under 35 U.S.C. 102(e),

it is respectfully submitted both Butler and Smeets clearly disclose the random numbers are to be

used in Cryptographic applications, and the generations of a chaos-based pseudo-random

sequence as disclosed in these references do not involve any truly random source but merely

based on arithmetic and logic operations, and thus clearly can be repeated. Therefore, the

generated sequences in Butler and Smeets are clearly a chaos-based pseudo-sequence as claimed.

8.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

9.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

10.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Chuong D. Ngo whose telephone number is (571) 272-3731. The

examiner can normally be reached on Monday-Friday.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Lewis, Jr. A. Bullock can be reached on (571) 272-3759. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Chuong D Ngo/
Primary Examiner, Art Unit 2193

12/07/2008